

REMARKS

This Amendment is filed in connection with a Request for Continued Examination and in response to the Final Office Action mailed July 16, 2007 and the Advisory Action mailed Oct. 2, 2007. The Applicant respectfully requests reconsideration. The objections and rejections are respectfully traversed.

Claims 1-28 are now pending in the case.

Claims 1, 14, 18, and 24 have been amended.

Claims 25-28 have been added.

Specification

At paragraphs 15-16 of the Final Office Action, the Examiner comments that “the trademark Cisco Systems has been noted on page 13 and 14 in the application” and requests it be accompanied by generic terminology.

The Applicant respectfully requests this be reconsidered. The Applicant refers to the corporation name “Cisco Systems, Inc.” on pages 13 and 14 of the specification. Referring to a corporation by name is quite different than using a term as a trademark. As such, the Applicant urges that the specification’s wording is proper.

Claim Rejections - 35 U.S.C. §101

At paragraph 17-18 of the Final Office Action, claims 18-23 were rejected under 35 U.S.C. §101. In the Advisory Action the Examiner indicates this rejection has been overcome.

Claim Rejections - 35 U.S.C. §102

At paragraphs 20-25 of the Final Office Action, claims 1-4, 14, 18, and 24 were rejected under 35 U.S.C. §102(e) over Roese, U.S. Patent Application No. 2004/0158735 (hereinafter Roese).

Roesse discusses a port-based authentication scheme that follows the IEEE 802.1X standard. A function is attached to a “network access port.” *See* paragraphs 0011. The “network access port” is associated with a “logical controlled port” and a “logical uncontrolled port.” *See* paragraphs 0011 and 0012. An authentication decision is rendered for the attached function. *See* Fig. 3, block 255. If the attached function is not authenticated, all communication proceeds through the uncontrolled logical port. *See* paragraph 0012. “Upon authentication of the attached function/supplicant, the logical controlled port is enabled and the supplicant is granted access to those network services provisioned to that network access port for the authenticated supplicant. As a result the attached function is not forced to reauthenticate unless as required under a proprietary network usage policy enforced by the network administrator.” *See* paragraph 0012.

Of note, Roesse envisions only one “attached function” attached to each port. The entire the port is basically switched between two states “controlled” and “uncontrolled” for use by that one “attached function.”

Problems occur with such an approach if multiple “attached functions” or devices are attached to a port, for example if the port were to operate as a “shared media port”. In such a case, one device could cause the port to switch to the “controlled” state while another device could “piggyback” on this access. The Applicant discusses this problem at length in the background section of the Application at page 6, lines 9-22 stating (emphasis added).

Network security problems often arise when both authorized and unauthorized users communicate through a shared media port that is configured to perform port-based network access control, such as 802.1X authentication. As noted, the shared media port transitions from an unauthorized to an authorized state once a user is authenticated at the port. ***Consequently, unauthenticated users at client nodes coupled to the shared media port may gain unauthorized access to the intermediate node’s services as soon as a user is authenticated at another client node coupled to that port.*** In this situation, network security may be compromised by the unauthenticated users coupled to the authorized port....Unfortunately, the IEEE 802.1X standard does not address the possibility of such security breaches at shared media ports.

The Applicant addresses shortcomings of prior approaches such as Roese. For example, the Applicant's claim 1, representative in part of the other rejected claims, sets forth:

1. A method for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being coupled to a plurality of client nodes, the method comprising:
 - partitioning the shared media port into a plurality of logical subinterfaces, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;
 - receiving a data packet at the shared media port from a first client node;
 - associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;
 - determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork;***
 - if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork;
 - receiving a second data packet at the shared media port from a second client node;
 - associating the second received data packet with the first logical subinterface;
 - determining whether the second client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork;*** and
 - if the second client node is determined to not be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, ***preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network of subnetwork, while still allowing data packets from the first client node to be forwarded if the first client node is determined to be authenticated.***

The Applicant respectfully directs the Examiner's attention to the limitations of "***determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork;***" and "***determining whether the second client node is authenticated to communicate over the first logical***"

subinterface's dedicated network or subnetwork” and “preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network of subnetwork, while still allowing data packets from the first client node to be forwarded if the first client node is determined to be authenticated.”

Rather than simply switching an entire port between two states (“controlled” and “uncontrolled”) for all devices attached to the port, the Applicant claims a technique where multiple client nodes are individually authenticated and can be maintained with differing access. Thus, the Applicant teaches “preventing the second received data packet from being forwarded ..., while still allowing data packets from the first client node to be forwarded.” The teachings of Roese would not permit such capability.

Accordingly, the Applicant respectfully urges that Roese is legally insufficient to anticipate the present claims under 35 U.S.C. §102 because of the absence of the Applicant's claimed novel *“determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork;”* and *“determining whether the second client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork”* and *“preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network of subnetwork, while still allowing data packets from the first client node to be forwarded if the first client node is determined to be authenticated.”*

Claim Rejections - 35 U.S.C. §103

At paragraphs 26-40 of the Final Office Action, claims 5, 8, 9, 11, 13, 15 17, 19 and 21-23 were rejected under 35 U.S.C. §103(a) over Roese in view of Kwan et al., U.S. Patent Application No. 2005/0055570 (hereinafter Kwan).

At paragraphs 41-47 of the Final Office Action, claims 6 and 10 were rejected under 35 U.S.C. §103(a) over Roese in view of Kwan, in further view of Ng. et al., U.S. Patent Application No. 2005/0177865 (hereinafter Ng).

At paragraphs 48-51 of the Final Office Action, claims 7, 16 and 20 were rejected under 35 U.S.C. §103(a) over Roese in view of Haverinen et al., U.S. Patent Application No. 2004/0208151 (hereinafter Haverinen).

At paragraphs 52-55 of the Final Office Action, claim 12 was rejected under 35 U.S.C. §103(a) over Roese in view Kwan and in further view of Inoue et al., U.S. Patent No. 6,891,819 (hereinafter Inoue).

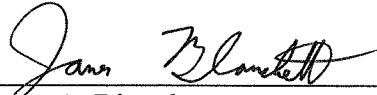
The Applicant notes that all of the claims rejected under U.S.C. §103 are dependent claims which depended from independent claims believed to be allowable. Accordingly, the dependent claims are also believed to be allowable for at least this reason as well as for other separate reasons.

Should the Examiner believe telephonic contact would be helpful in the disposition of this Application, the Examiner is encouraged to call the undersigned attorney at (617) 951-2500.

In summary, all the independent claims are believed to be in condition for allowance and therefore all dependent claims that depend there from are believed to be in condition for allowance. The Applicant respectfully solicits favorable action.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,


James A. Blanchette
Reg. No. 51,477
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500